

CRYA – A SECURE MESSAGING APPLICATION

Prachi Jogdand, Asawari Kale, Sarvesh Tiwari, Saiyed Mayoof Prof. Swati Gaikwad

Bachelor's Degree in Computer Engineering AIML & Bharat College of Engineering

ABSTRACT: Nowadays, communication through. The use of messaging apps is now widespread. However, Numerous applications lack complete security measures. And user privacy. The risk of data leakage is never exempt. Hacking, or unauthorized access. To solve this problem, we. Established CRYA, a password-protected messaging app that emphasizes encryption. The company is. On protecting user data. The application uses encryption. Strategies to ensure the safety of transmission. Messages are read by only the sender and. It also has features such as self-contained, secure login and so on. Destruct messages, and private communication. The main aim. CRYA's goal is to offer a secure and uncomplicated platform for users to make changes. Communicate without worrying about privacy.

I. INTRODUCTION

With the emergence of messaging apps, communication has become more accessible and efficient in the digital era. These platforms are utilized by individuals for facilitating personal discussions, professional interactions, and sharing important data. WhatsApp, Telegram, and other apps have made instant messaging a common feature in everyday lives. What are some examples?

In addition to convenience, there are now concerns about the security of data and user privacy. There are various messaging platforms that hold user information on servers, monitor user activity or expose them to cyber attacks. This may cause significant problems such as data breaches, unauthorized access, and the misuse or exploitation of personal information.

There needs to be a messaging system that balances security and privacy with user-friendliness in solving these issues. CRYA – A Secure Messaging Application is the key factor in this.

Modern encryption methods are utilized in CRYA to ensure secure communication. The app takes care of converting messages into non-readable text and only allows the intended recipient to read them. This prevents the server and other third parties from accessing the messages.

2. Body of Paper

Numbered sections and of the body, which are the main findings. The content should be emphasized the most in the arrangement of these parts.

Retracting (or elaborating) on particular sections is often essential. Such references also contain the section number, as in "In Sec." (Ex. 2. During the phrase, these words can be combined to form Sec, Ref. (for instance), Eq. or Fig.

When an acronym is introduced, spell it out and attach the acronym in brackets, like CCD.

1.1 Project Plan

A systematic approach is taken to ensure the delivery of a reliable and efficient secure messaging application, such as the CRYA one. During the first step, a thorough assessment of requirements is conducted to determine the necessity for secure communication and data privacy, as well as to protect against unauthorized access. The system design is based on these requirements, which includes the establishment of the system architecture, direction of data flow, and selection of necessary technologies such as frontend frameworks, backend services, encryption methods, etc.

Following this, the implementation process starts, where different modules like user authentication, message encryption techniques, secure data transmission methods and user interface are created (and then integrated).. This includes special attention to encryption algorithms for protecting the confidentiality of messages. After the system is developed, it is subjected to extensive testing (functional testing, security testing) in order to identify any bugs or vulnerabilities.

Once the system is tested successfully, it is deployed for practical use. Finally, the system enters the maintenance phase, where performance is monitored and future enhancements such as improved security features, better scalability, and additional functionalities are planned to make the application more efficient and user-friendly

II . Review of Literature

Many secure messaging systems have already been developed. For example, WhatsApp uses encryption, but it still collects user data like metadata. Telegram provides both normal and secret chats, but not all chats are fully encrypted. Signal is known for strong security, but it has limited features and flexibility.

From studying these systems, it is clear that there is still a need for an application that provides both strong security and user-friendly features. CRYA is designed by considering these gaps.

2.1 Existing Systems

- Presently, WhatsApp, Telegram, and Messenger are among the most commonly used messaging apps. The messaging services offered by these platforms are fast and simple, including text messaging as well as media sharing and voice communication. Nevertheless, they are widely used and possess numerous constraints in terms of security as well as privacy.

One of the primary challenges with current systems is the fact that centralized servers are often utilized to store user data. In some cases, the data is still accessible under certain conditions, especially metadata such as user activity, contact details, and timestamps, despite applications that claim to use encryption. The risk of data misuse is present. End-to-end security is not fully implemented in certain applications, posing another problem. While certain platforms.

- Providing encryption is not always the case in every form of communication. The lack of complete encryption in cloud-based chats can make them susceptible to hacking attempts.

Hacking, phishing attacks, and data breaches are among the cyber threats that exist on existing systems. Why? A server attack can expose user sensitive data.? Concerns regarding data protection and confidentiality arise from this. Moreover, numerous applications monitor user behavior and actions, which impacts user privacy. Personal information is frequently left unsecured and the storage or utilization of it is not clearly defined.

Moreover, there are no advanced privacy features available, such as anonymous messaging or automatic message deletion. The risk of data exposure is high, as most applications store chat history on their storage unless manually deleted.

Because of these disadvantages, existing messaging systems are not entirely secure when it comes to communicating with users. For this reason, CRYA is an appropriate solution that prioritizes strong encryption, user privacy, and secure data management.

2.2 Literature Survey of Similar Ideas

- Numerous research endeavors and current applications have centered on secure communication methods as well as data protection techniques. These systems primarily function to offer privacy and secure communication through encryption.?

End-to-end encryption is used by WhatsApp, an application that is widely used. What are the implications of this? But research has revealed it still gathers metadata, including user activity and contact details, which can lead to privacy concerns.

Telegram is a well-liked platform that provides access to both regular and covert conversations. Unlike full encryption, secret chats are stored on the cloud and not in any way secure.

Strong encryption protocols and the absence of user data storage make Signal one-of-a-kind messaging applications regarded as highly secure. The interface is simple and it has some limitations, resulting in less adoption.

AES (Advanced Electromagnetic Shielding) is believed to be a useful combination of encryption techniques, according to research papers on secure communication.

- Encryption Standard and RSA can enhance data security significantly. The former is used for encryption, while the latter is not yet implemented. Many systems also place great emphasis on user authentication and secure key exchange.

The analysis of current systems and research results indicate that security measures are being implemented, but there are still gaps in terms of complete privacy, user control, and other security features.

Accordingly, the proposed CRYA system was created to overcome such shortcomings: strong encryption; better control of privacy; and more user-friendly features in one platform.

III. Proposed System

CRYA – A Secure Messaging Application is the proposed system designed to provide users with a secure and private messaging platform. This system is designed to ensure that no- one can read them and that they are not leaking sensitive information.

The CRYA encryption method employs end-to-end encryption to prevent the transmission of messages and ensures that they are not unreadable and can only be returned to their original format by the intended recipient. Intercepting data does not make it incomprehensible to third parties.

Additionally, a secure authentication mechanism is included in the system to authenticate users. Methods such as passwords or OTP are available for users to log in and help prevent unauthorized access to accounts.

Traditional messaging systems require more server-side data storage than CRYA. This is mainly used as a server to send encrypted messages, not to store read data. By reducing the risk of data leakage, security is improved.

The system aims to provide a user-friendly and secure interface. CRYA's approach to communication surpasses that of existing messaging apps by utilizing encryption techniques, secure authentication, and privacy-focused features.

3.1 Analysis/Framework/Algorithm:

Step1: User Authentication.

The problem is that the system can be accessed by users who are authorized. Solution: Establish secure login by means of password,OTP, or biometric authentication to authenticate users.

Step 2: Key Generation.

The challenge: Communication must be managed effectively.. Method: Create public and private keys (e.g, RSA) to exchange secure data./method of encryption?

Step 3: Message Encryption.

The difficulty: Plain text messages can be intercepted while being sent.
Use AES encryption to encrypt messages and send them over the network.

Step 4: Secure Data Transmission.

Problem: Data may be exposed when transmitted across networks. Eliminate any readable data by transmitting only encrypted messages through a secure server.

Step 5: Message Decryption.

Challenge: Encrypted messages must be read again to be readable by users. Decrypting the message with the private key of the receiver will reveal the original content.

Step 6: Data Storage.

Data leakage occurs when messages are stored on servers. To avoid permanently storing sensitive data, it is recommended to only store encrypted or limited amounts of data.

Step 7: Privacy Features.

Obstacle: Users require greater authority over their data and conversations.

Remedy: Add features such as self-destruct messages and anonymous chat for more privacy.

Step 8: Security and Performance.

Challenge: Safe and fast. What is the problem? Solution: Encrypting data efficiently with an optimized backend for fast and secure communication.

3.2 System Architecture (Challenges of Sentiment Analysis Tool)**1. Data Security.**

Problem: Messages can be intercepted during transmission, leading to data leakage.

The solution is to encrypt the messages from end to end, making them unreadable to third parties. This method is recommended.

2. Key Management.

Issue: If the encryption keys are handled incorrectly it can pose security risks.

Use secure key generation and exchange solutions such as RSA or Diffie-Hellman.

3. Server Vulnerability.

Centralized servers are vulnerable to attacks.

Encrypting the data on servers is necessary to minimize risk, and limiting storage space is an alternative.

4. User Authentication.

Problem: Accounts could be accessed by anyone who is not authorized.

Strengthen authentication methods such as OTP, passwords or biometric verification.

5. Data Privacy.

The concern is the potential for misuse or unauthorized access of user information, such as messages and personal data.

Answer: Collect less data, collect more data encrypted?

6. Performance and Speed.

Problem: Encryption processes can lead to a decrease in the speed of message delivery.

Utilizing efficient algorithms (AES) and optimized backend systems to maintain fast communication is the solution.

7. Message Storage.

The danger of storing messages permanently is that it increases the risk of data leakage.

Solution: Take temporary storage and self-embedded messages.

8. User Experience.

High security systems can be complicated for users. Why? -

The solution: Create a user-friendly interface with adequate security measures.

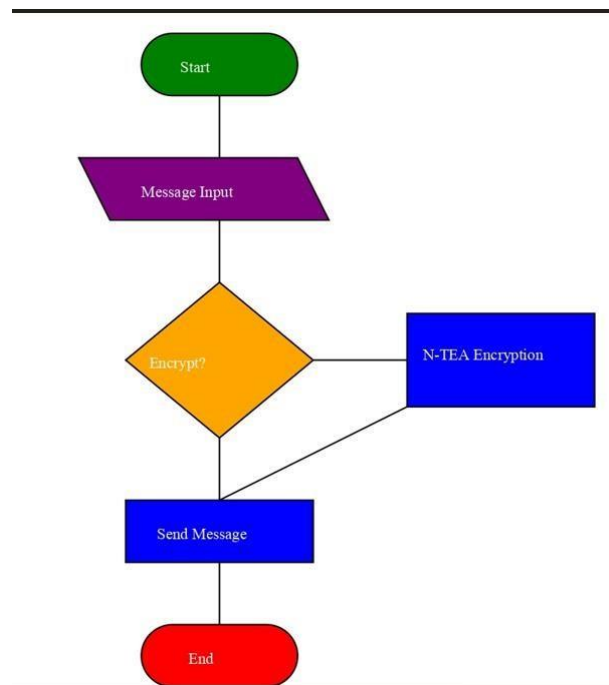


Fig 3.2.1 FLOW CHART

3.3 Data Model:

Data Model.

The CRYA secure messaging system employs a data model that provides guidelines for data storage, management, and security.

User Profile:

Contains user information like username, email address and password for authentication purposes.

Message Data:

Encompasses the encrypted messages exchanged among users. Text messages are not legible and therefore, cannot be read.

Encryption Keys:

Secures public keys and private keys for encryption and decryption.

Chat History:

Keeps confidential conversations in either encrypted or temporary storage.

Media/Data Files:

Stores shared files (images/documents) in encrypted format to ensure security.

3.4 Methodology:

The CRYA system is designed to safeguard communication:

User Authentication:

Password or OTP verification is among the secure methods users can use to log in.

Key Generation:

It generates both public and private keys to ensure safe communications.'

Message Creation:

Using the application interface, the sender can compose a message.

Encryption Process:

AES/RSA encryption is employed before the transmission. Why?

Secure Transmission:

The original data remains unreturned as the encrypted message is transmitted through the server.

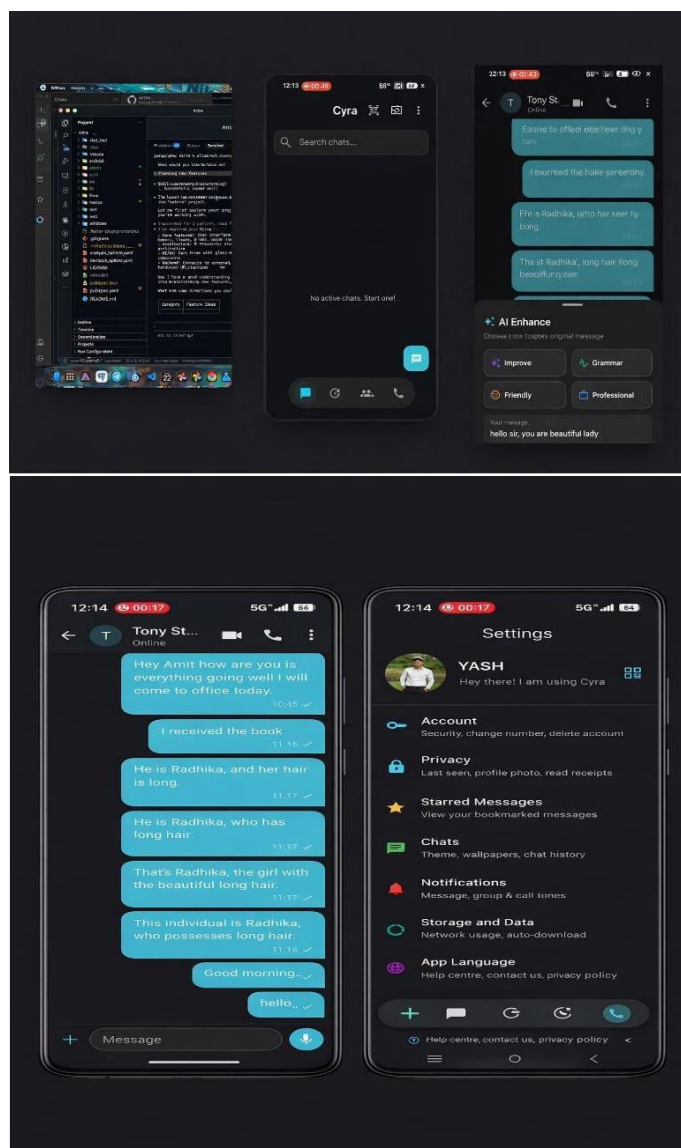
Message Decryption:

The message is decrypted by the recipient through a private key.

Data Handling:

To ensure privacy, only encrypted or limited amounts of data are stored.

IV. Proposed System Result:



V. Conclusion:

CRYA, A Secure Messaging Application, seeks to provide a secure and reliable communication platform by taking advantage of the significant drawbacks of current messaging systems. The application employs end-to-end encryption to safeguard user messages and maintain their confidentiality.

During message delivery, the system ensures data confidentiality, integrity, and security measures. The inclusion of secure authentication, encrypted messaging, and limited data storage enhances the overall user's privacy and reduces potential data leakage.

The application is also designed to be user-friendly and secure. This makes it a good choice for both personal and professional communication.

Future enhancements to the system include multi-device support, AI-based threat mitigation (see below), and other advanced features.

Detection, and enhanced performance optimization. CRYA is a practical solution for ensuring secure communication in the digital age.

References:

1. Stallings, W., (2017). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
2. Kahn Academy, (2022). *Introduction to Cryptography and Secure Communication*.
3. Rescorla, E., (2001). *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley.
4. Green, M., & Smith, M., (2016). "The Cryptopals Crypto Challenges." *Cryptography Research Papers*.
5. Dierks, T., & Rescorla, E., (2008). "The Transport Layer Security (TLS) Protocol." IETF RFC 5246.
6. OpenSSL Project, (2023). *OpenSSL Cryptography Library Documentation*. Retrieved from <https://www.openssl.org>
7. **Title:** New Directions in Cryptography **Authors:** Whitfield Diffie, Martin Hellman **Year:** 1976
8. **Title:** WhatsApp Encryption Overview **Company:** WhatsApp

Acknowledgment:

We would like to acknowledge and thank our project mentor (Swati Gaikwad) for their unwavering commitment, guidance, and support during this challenging journey. The work was accomplished with the help of their insights and suggestions.

We acknowledge the contribution of the faculty members in the Department of Computer Engineering for providing us with the necessary resources and knowledge.

Lastly, we want to acknowledge and thank our loved ones for their unwavering support and encouragement during this research endeavor.

Android Developers, (2023).

Android Security and Encryption Guide. Retrieved from <https://developer.android.com>.

OWASP Foundation, (2023). *Mobile Security Testing Guide (MSTG)*. Retrieved from <https://owasp.org>.

BIOGRAPHIES

Prachi Jogdand “currently pursuing a Bachelor of Engineering in Artificial Intelligence and Machine Learning from Bharat College of Engineering, Maharashtra, India. She is interested in secure communication systems, machine learning, and Python programming. Her research interests include data security, encryption techniques, and secure messaging applications”.

Asawari Kale “pursuing a Bachelor of Engineering in Artificial Intelligence and Machine Learning from Bharat College of Engineering, Maharashtra, India. She has an interest in software development, cybersecurity, and artificial intelligence applications. Her research interests include secure systems, data protection, and web-based applications”.

Sarvesh Tiwari “currently pursuing a Bachelor of Engineering in Artificial Intelligence and Machine Learning from Bharat College of Engineering, Maharashtra, India. His interests include machine learning, data security, and Python programming. His research focuses on encryption methods, secure communication, and privacy systems”.

Saiyed Mayoof “pursuing a Bachelor of Engineering in Artificial Intelligence and Machine Learning from Bharat College of Engineering, Maharashtra, India. He is interested in software development, cybersecurity, and AI- based applications. His research interests include data security, secure messaging systems, and application development”.